

100

FIGURE 1

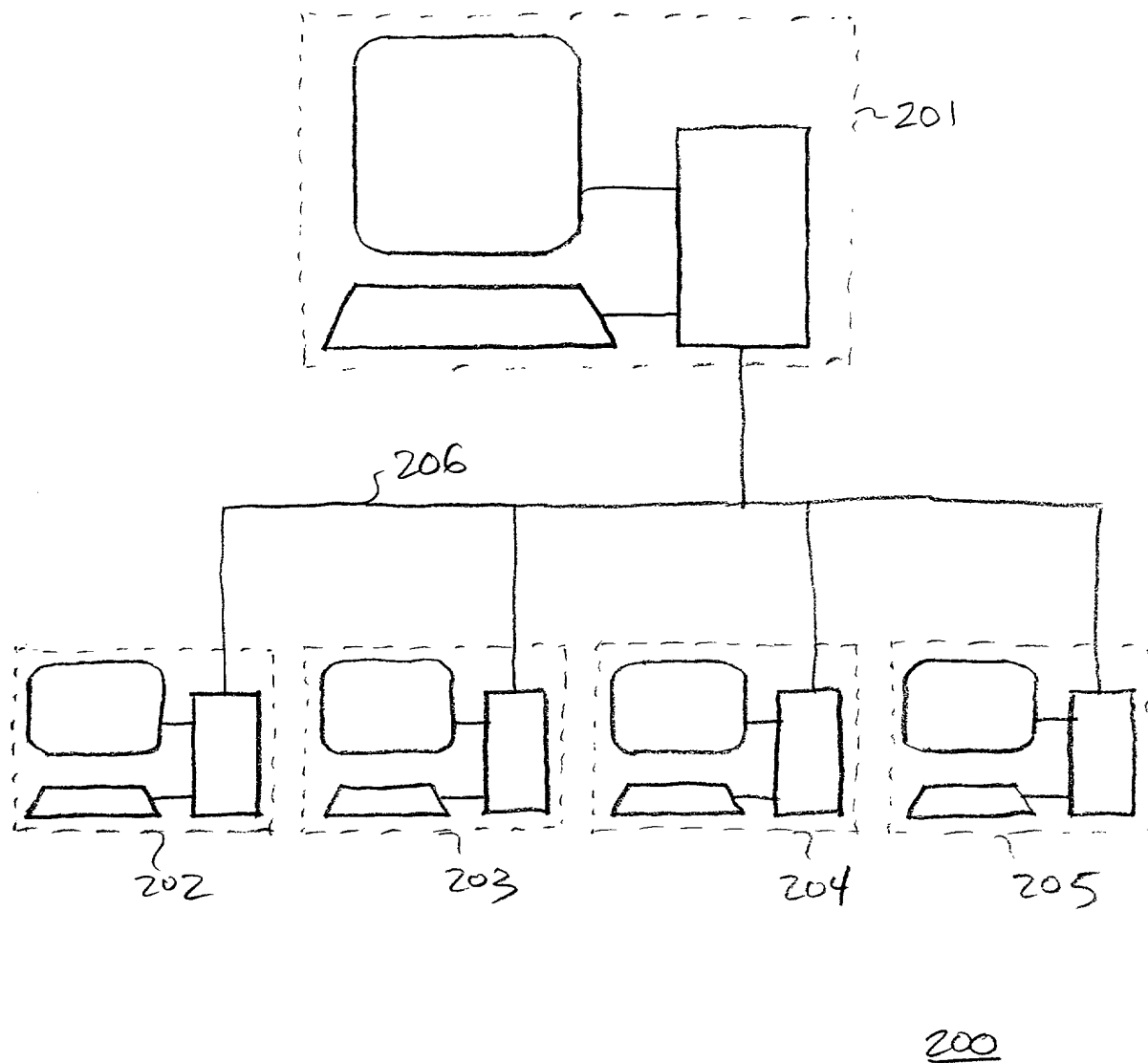
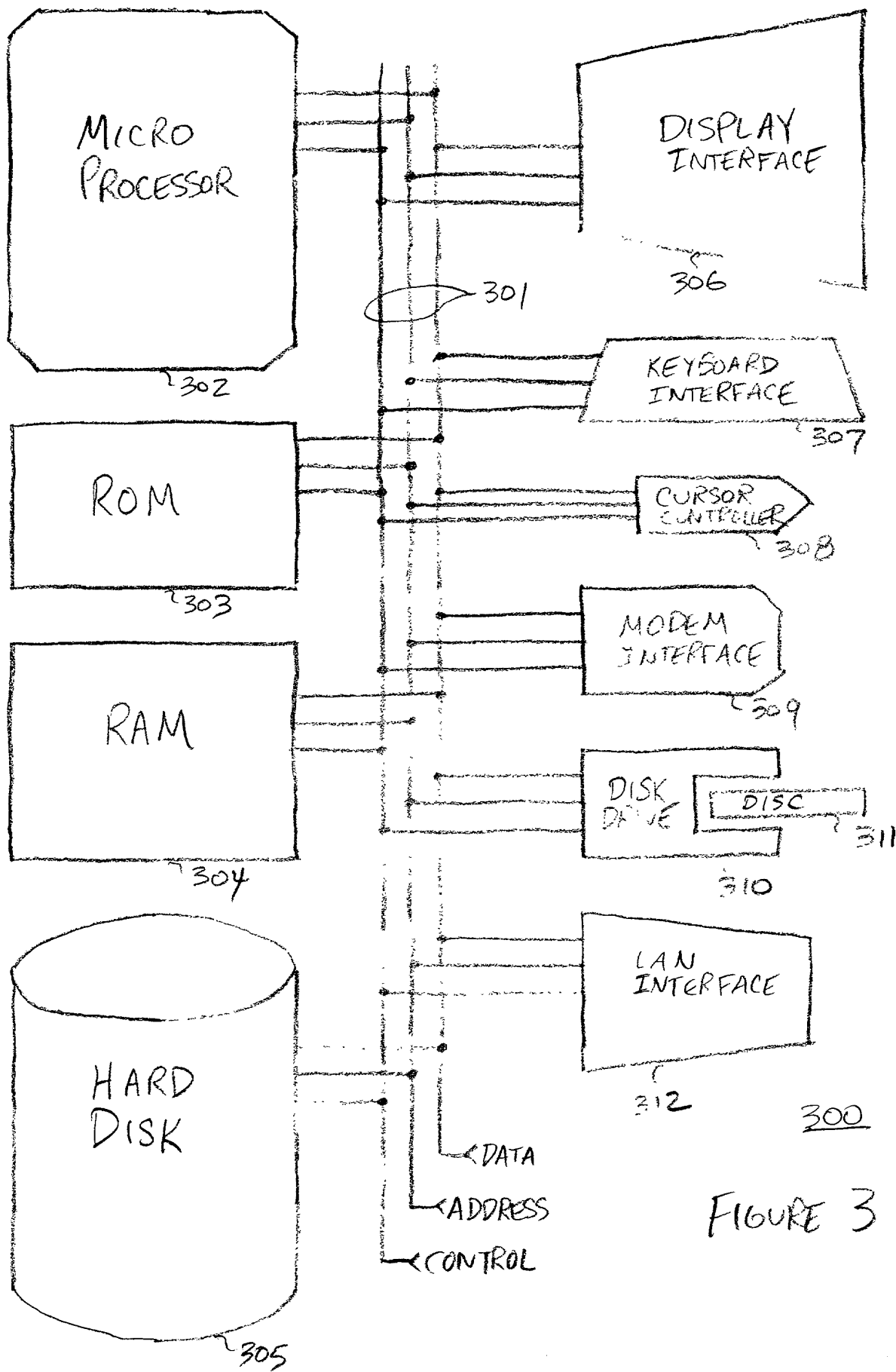


FIGURE 2



09859913 054404

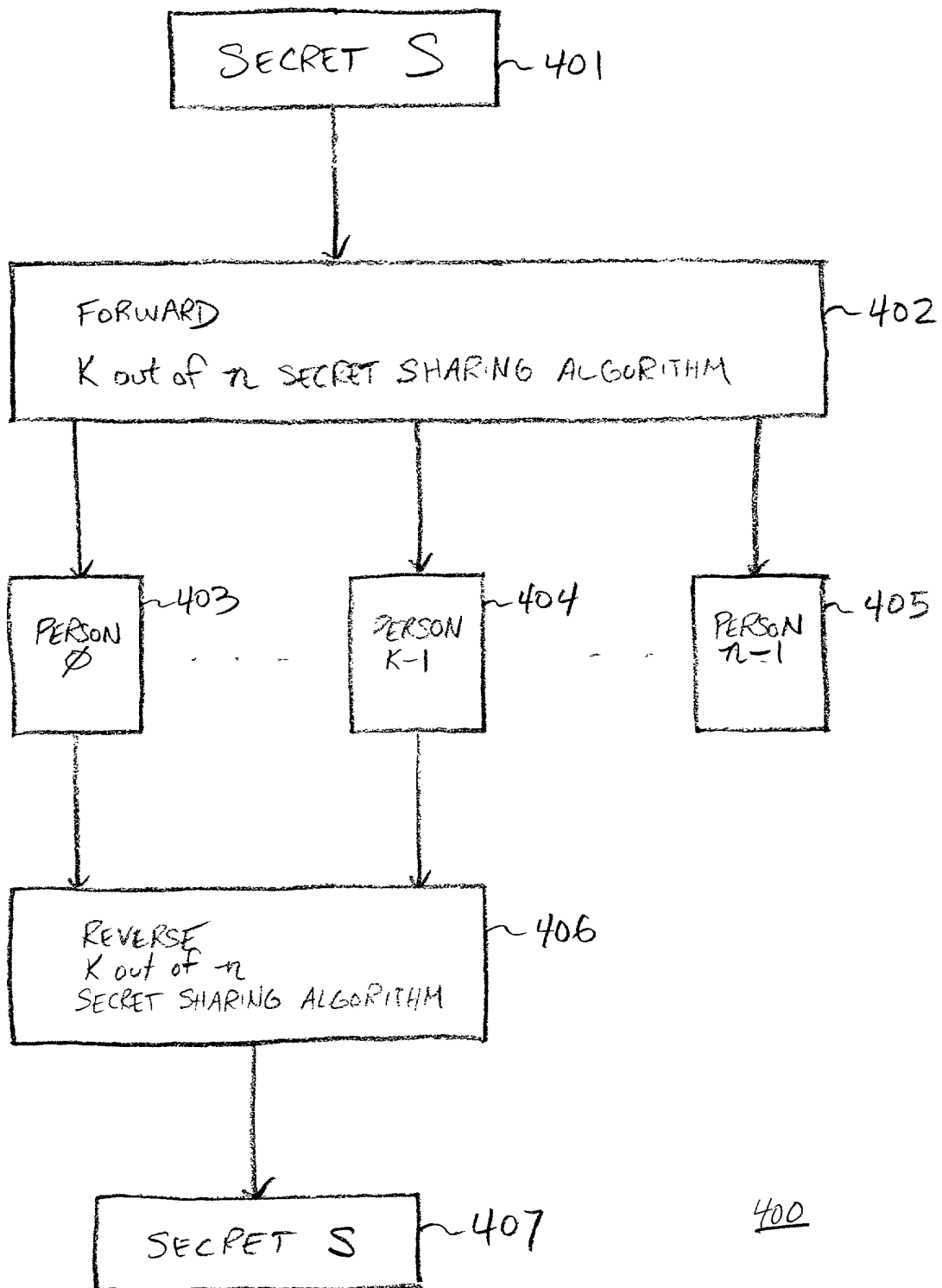


FIGURE 4

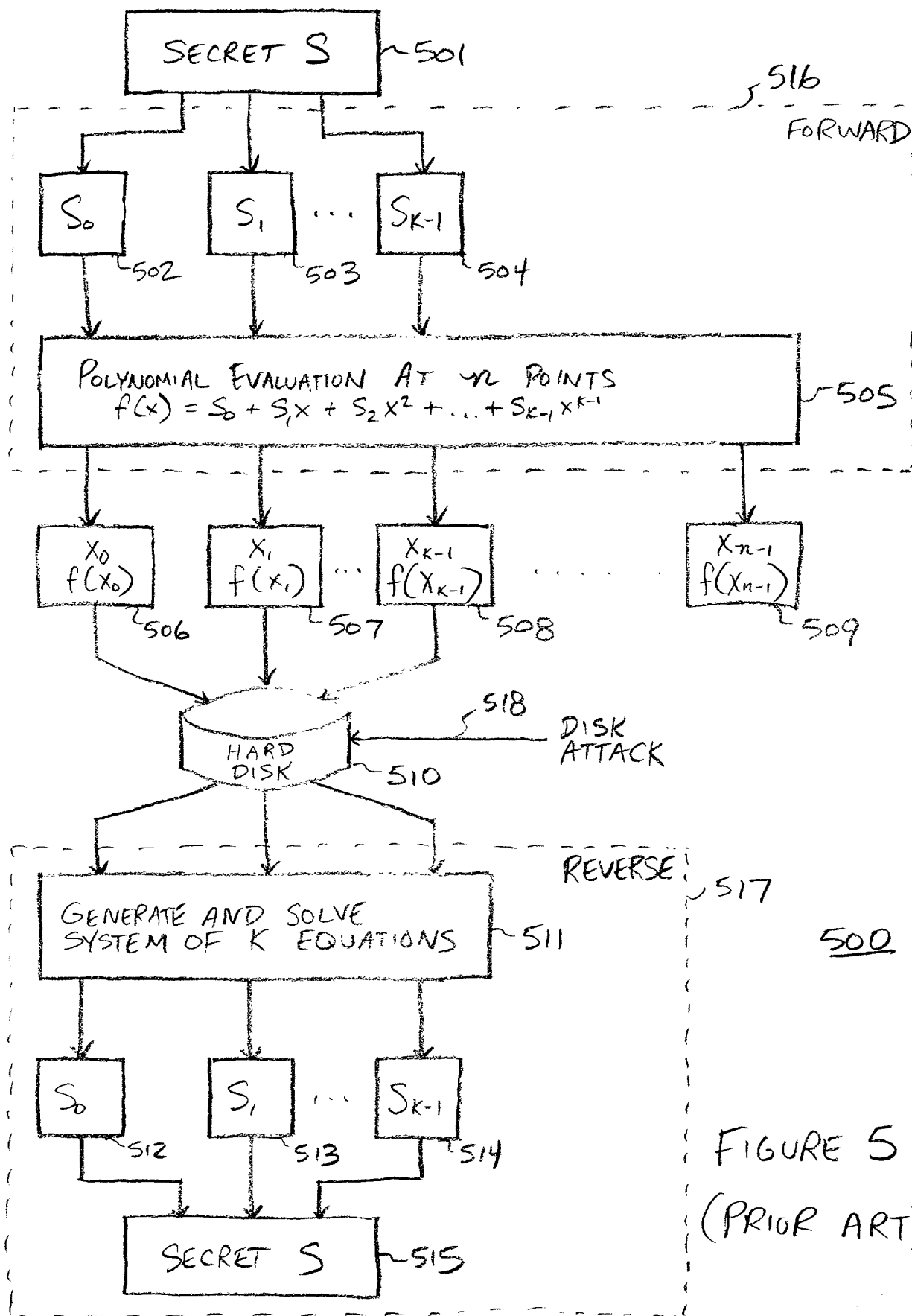
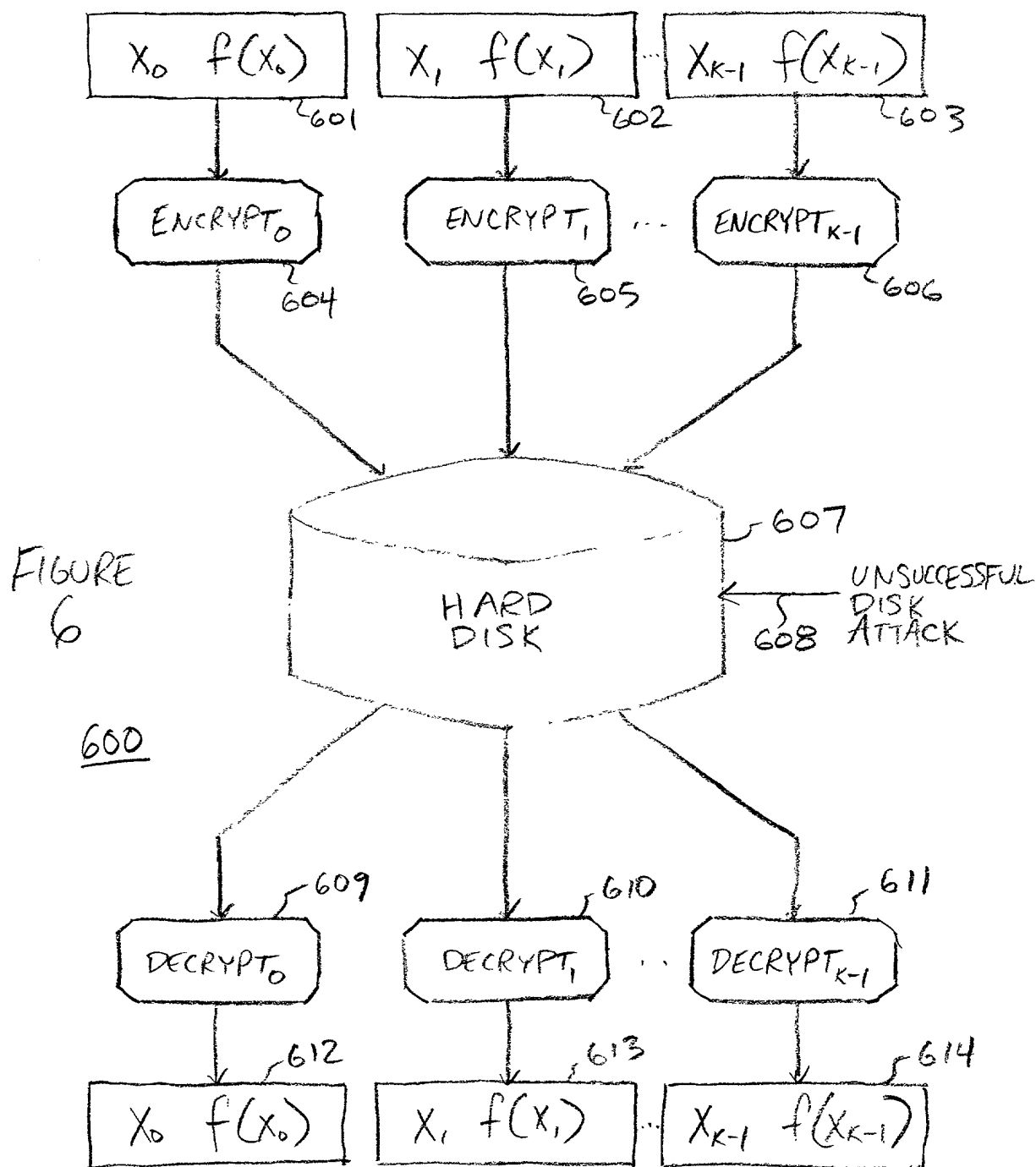


FIGURE 5
(PRIOR ART)



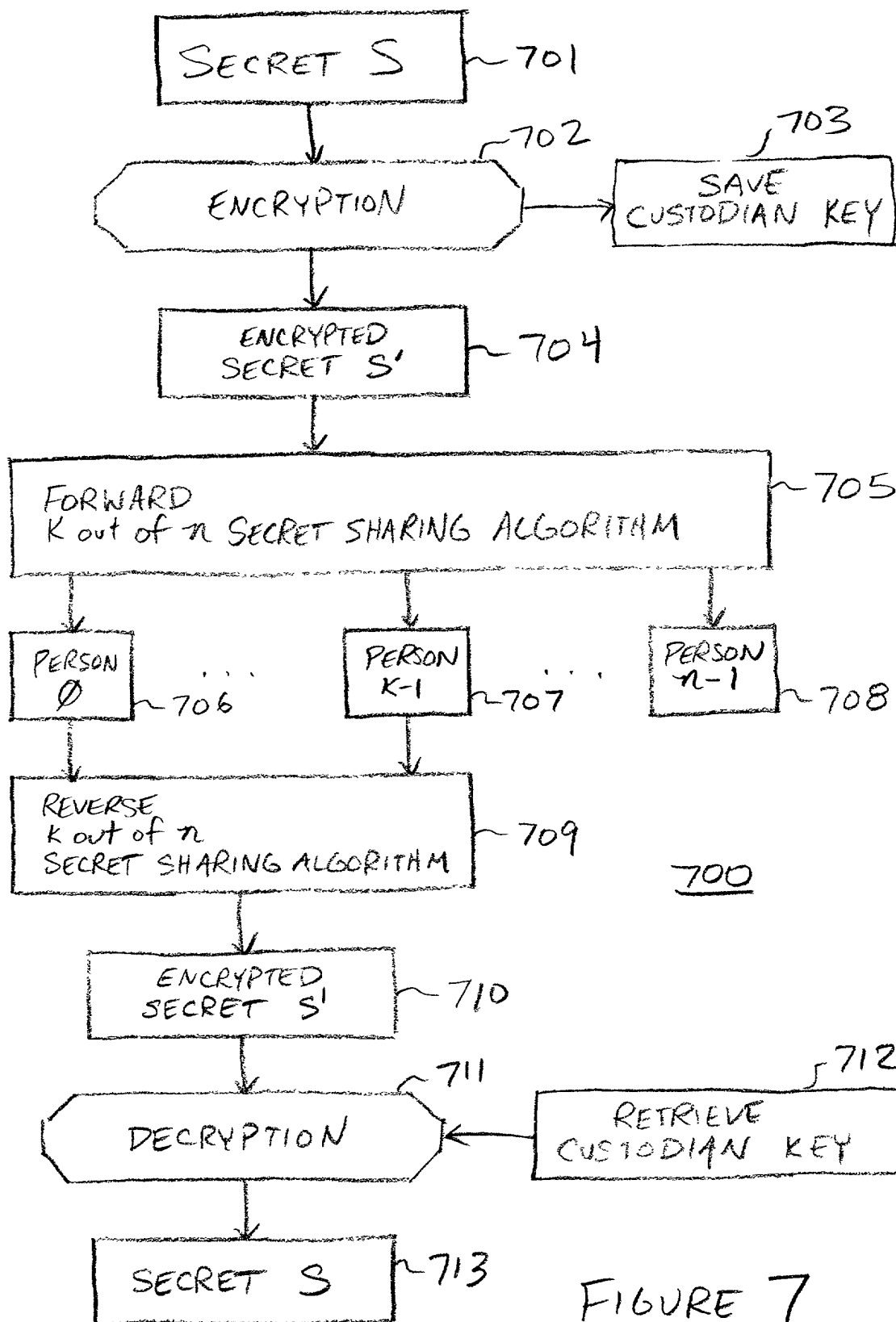
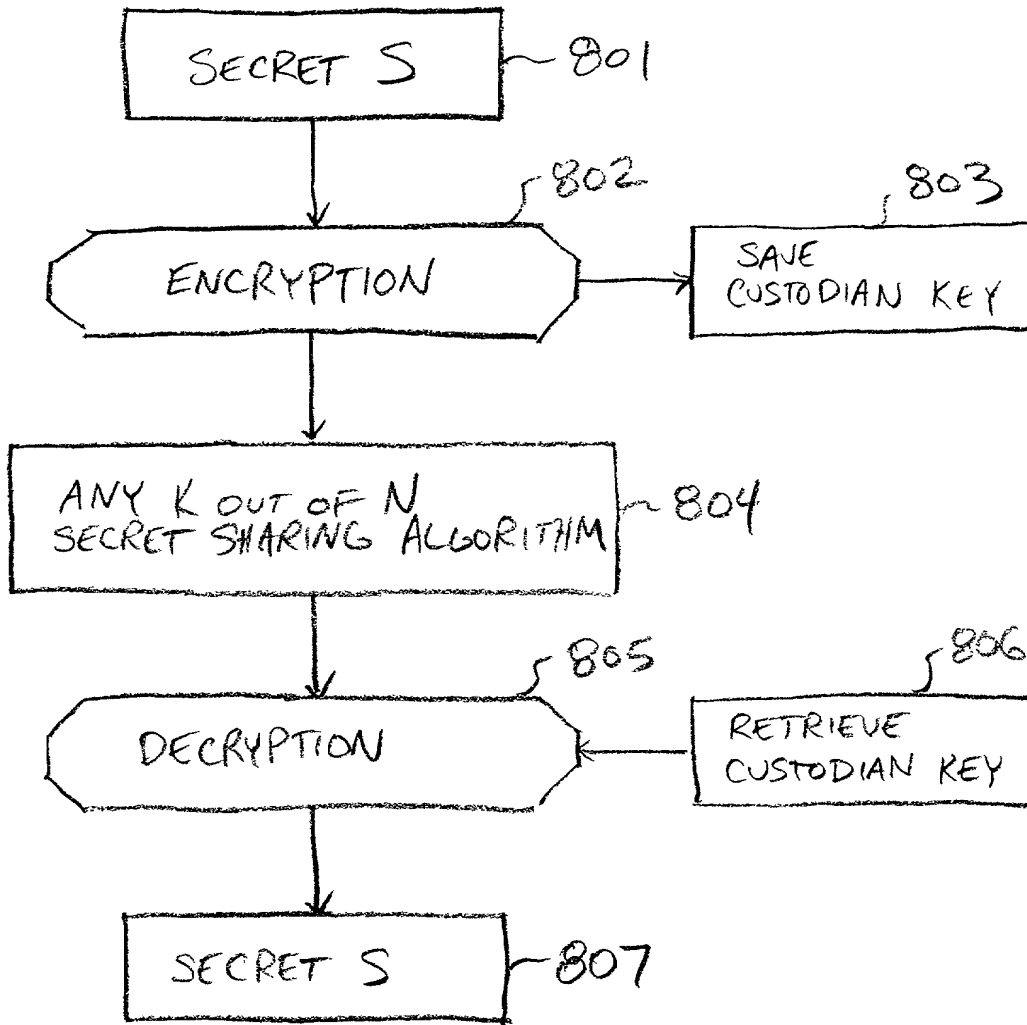


FIGURE 7



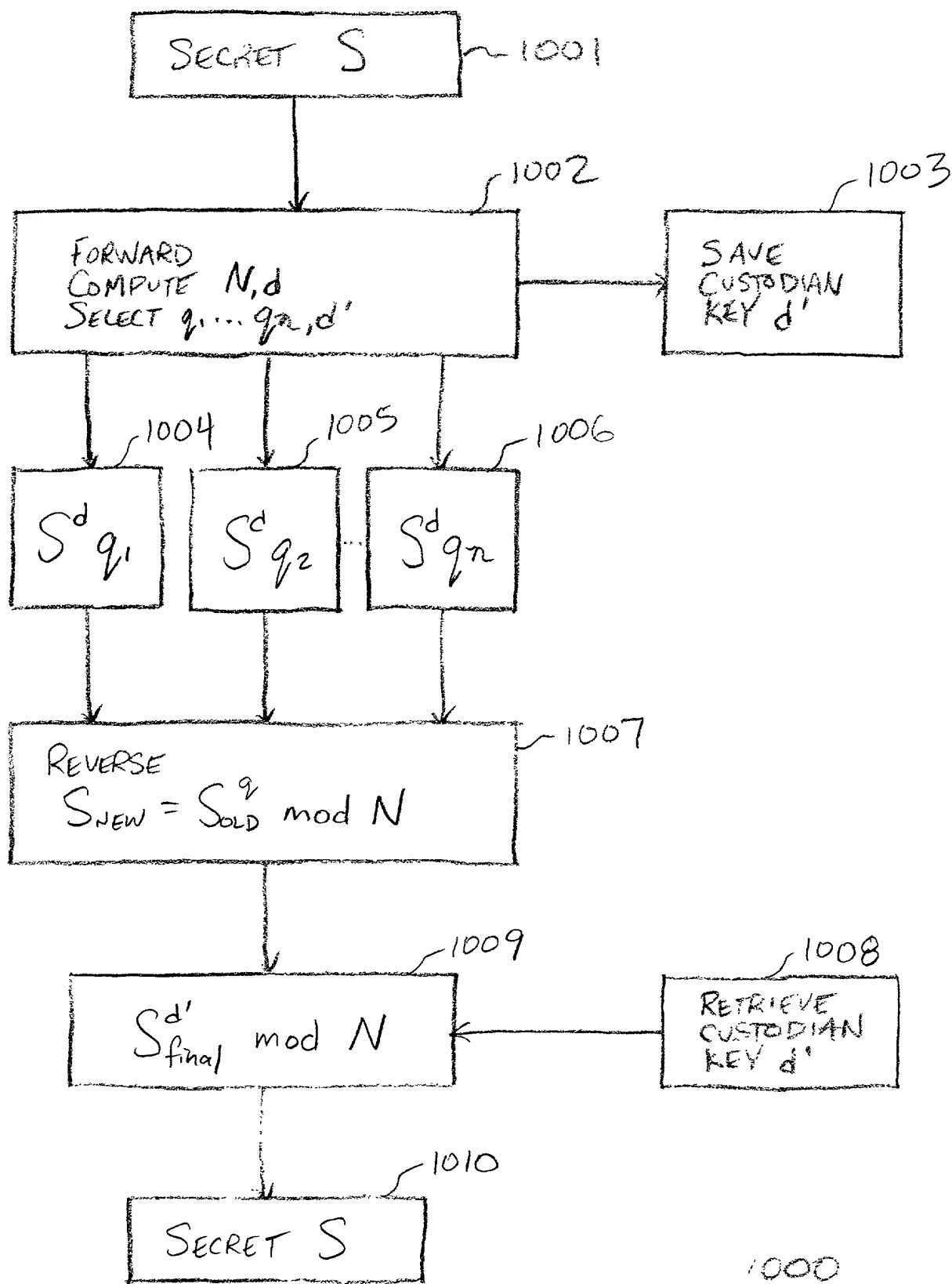
800

FIGURE 8


```
graph TD; A[SECRET S ~901] --> B[FORWARD  
COMPUTE N, d  
SELECT q1...qn ~902]; B --> C[S^d q1 ~903]; B --> D[S^d q2 ... ~904]; B --> E[S^d qn ~905]; C --> F[REVERSE  
S_NEW = S_OLD^q mod N ~906]; D --> F; E --> F; F --> G[SECRET S ~907];
```

The flowchart illustrates the reverse operation of a cryptographic system. It begins with a box labeled "SECRET S" with a tilde and "901". An arrow points down to a box labeled "FORWARD" with "COMPUTE N, d" and "SELECT q₁...q_n" and a tilde and "902". From this box, three arrows point down to three separate boxes: "S^d q₁" with a tilde and "903", "S^d q₂ ..." with a tilde and "904", and "S^d q_n" with a tilde and "905". Arrows from these three boxes point down to a box labeled "REVERSE" with "S_{NEW} = S_{OLD}^q mod N" and a tilde and "906". An arrow from this box points down to a final box labeled "SECRET S" with a tilde and "907".

FIGURE 9



1000

FIGURE 10

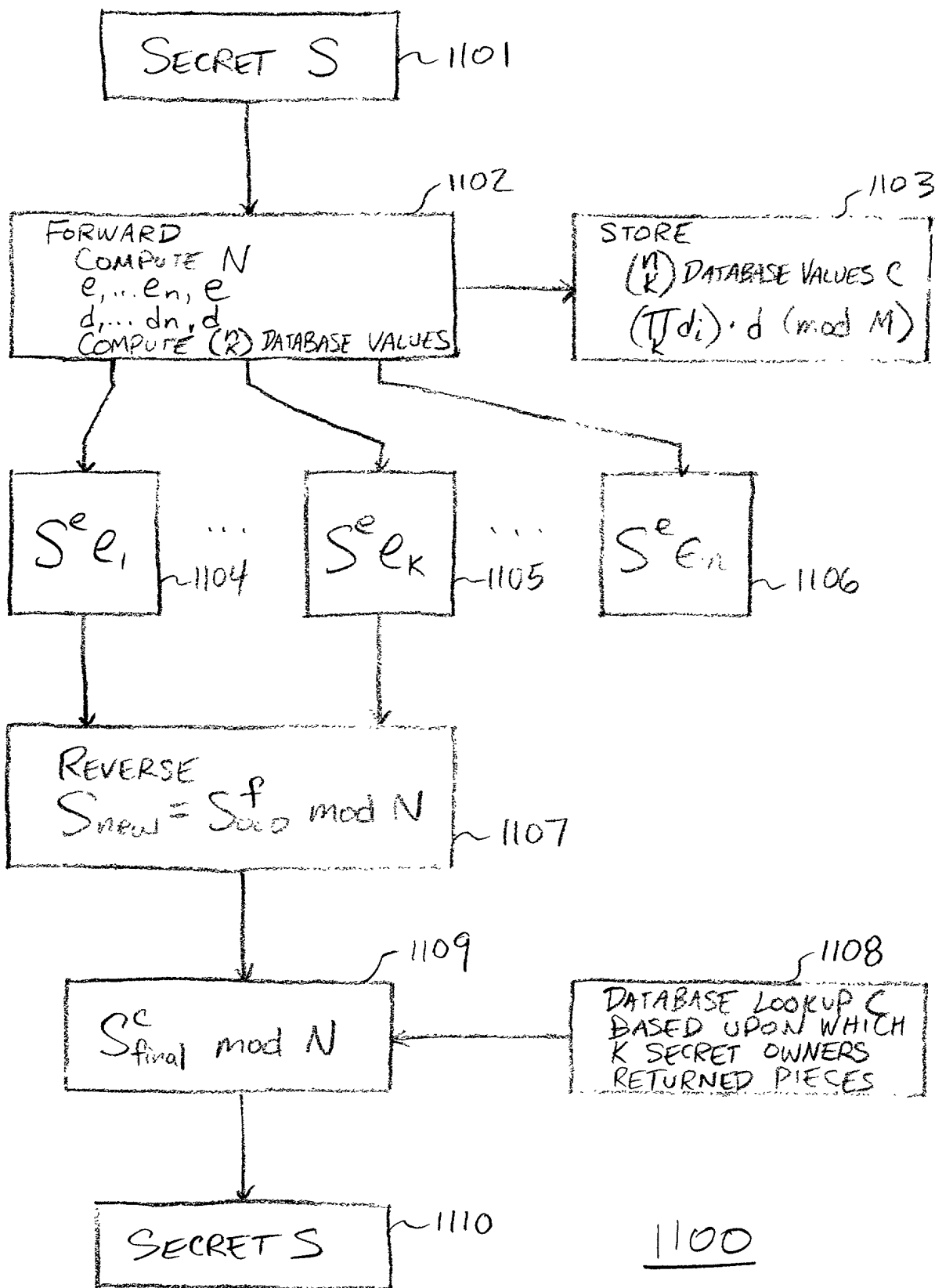


FIGURE 11

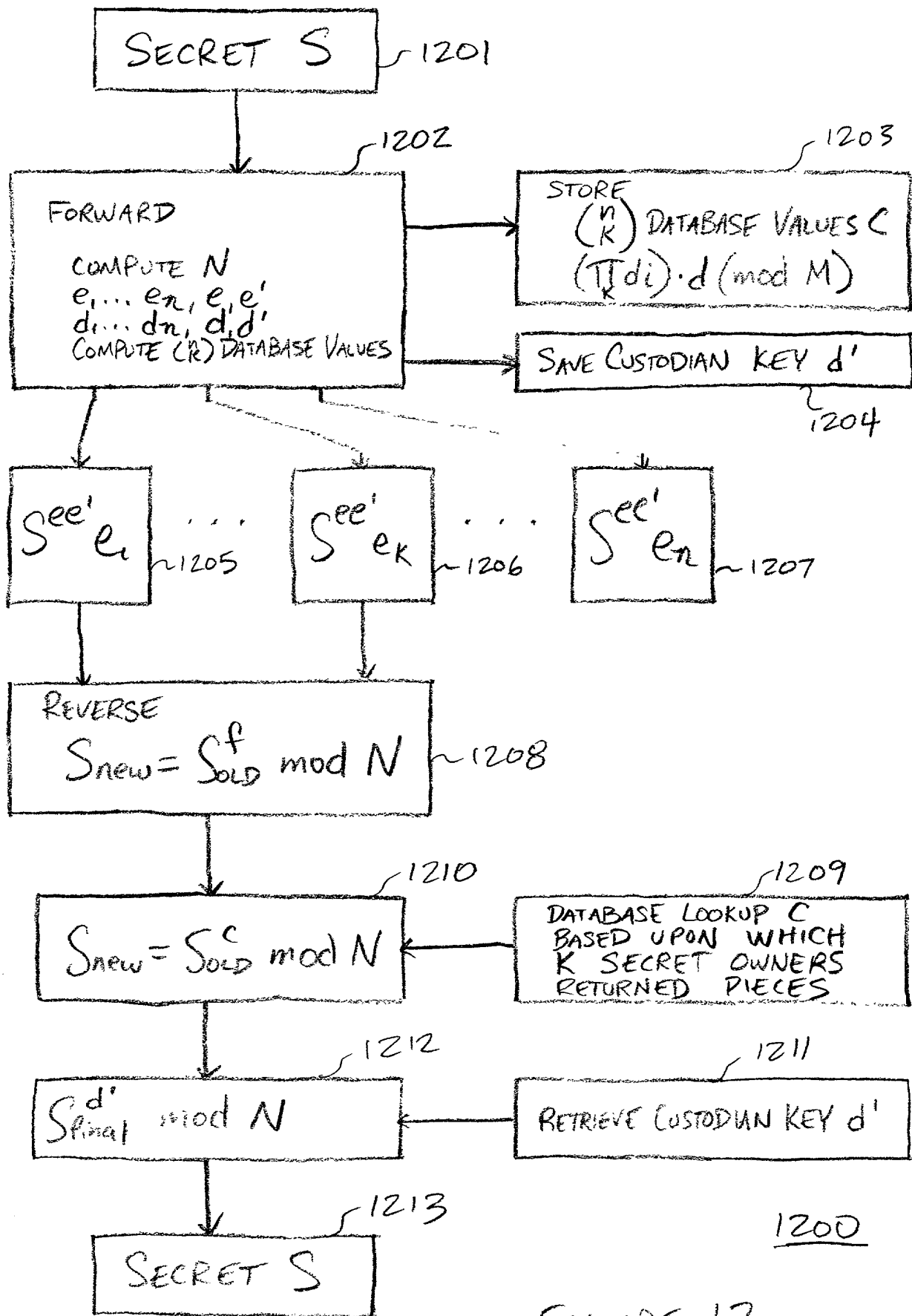


FIGURE 12